MARK J. BOURASSA, ESQ. (NBN 7999)
JENNIFER A. FORNETTI, ESQ. (NBN 7644)
VALERIE S. GRAY, ESQ. (NBN 14716)
THE BOURASSA LAW GROUP
2350 W. Charleston Blvd., Suite 100
Las Vegas, Nevada 89102
Telephone: (702) 851-2180
Facsimile: (702) 851-2189
Email: *mbourassa@blgwins.com*
jfornetti@blgwins.com
vgray@blgwins.com

GARY F. LYNCH (*pro hac vice forthcoming*)
PATRICK D. DONATHEN (*pro hac vice forthcoming*)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: (412) 322-9243
Email: *gary@lcllp.com*
patrick@lcllp.com

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA
***

OLIVER MCCUSKER, on behalf of himself and all others similarly situated, Plaintiff, v. CAESARS ENTERTAINMENT, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff OLIVER MCCUSKER ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated, against Defendant CAESARS ENTERTAINMENT, INC., ("CAESARS" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

/ / /

NATURE OF THE ACTION

1. Plaintiff brings this class action against CAESARS for its failure to properly secure its customers' sensitive personally identifiable information, including their names, driver's license numbers, and Social Security numbers (collectively, "PII"), and for failing to comply with industry standards to protect information systems that contain PII. Plaintiff seeks, among other things, damages, orders requiring CAESARS to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like this from reoccurring in the future, and for CAESARS to provide identity theft protective services to Plaintiff and Class Members for their lifetimes, as Plaintiff and Class Members will be at an increased risk of identity theft due to the conduct of CAESARS described herein.

2. CAESARS identifies itself as "the global leader in gaming and hospitality. While each of our over 50 world-class resorts offer its own unique amenities, all share a common goal of providing unparalleled family-style service and exhilarating experiences."[1] CAESARS's portfolio encompasses some of the most recognized resort brands in the industry, including Caesars Palace, Harrah's Las Vegas, Flamingo Las Vegas, The Linq, The Cromwell, Paris Las Vegas and Planet Hollywood along the Las Vegas, Nevada Strip.[2]

3. In the course of providing customers with gaming and hospitality services, CAESARS requires customers to entrust it with their highly sensitive personal information. In turn, CAESARS comes into possession of and maintains files containing the PII of its customers and has a resulting duty to securely maintain such information. As part of its business operations, CAESARS engages Okta, Inc. ("Okta") to provide it with identity and access management services.

4. Despite CAESARS's duty to safeguard the PII of its customers, cybercriminals gained access to CAESARS's loyalty program database on or about August 18, 2023, and later exfiltrated the sensitive PII stored therein (beginning on or about August 23, 2023) (the "Data Breach").[3] On or about

---

[1] *This is Caesars: Who We Are*, https://www.caesars.com/corporate (last visited Oct. 27, 2023).
[2] *Caesars Properties*, https://investor.caesars.com/caesars-properties (last visited Oct. 27, 2023).
[3] *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/b21dc5d1-0bee-4a4c-92dc-bef4bbb519c9.shtml (last accessed Oct. 27, 2023).

September 7, 2023, CAESARS confirmed that customer PII was exfiltrated from Defendant's computer systems.[4]

5. Based on CAESARS's statements to date, a wide variety of customer PII was implicated in the Data Breach, including names and driver's license numbers, and Social Security numbers.[5]

6. As a direct and proximate result of CAESARS's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of cybercriminals.

7. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, and similar forms of criminal mischief, which risk may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, energy, and money to protect themselves, to the extent possible, from these crimes.

8. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence, breach of implied contract, violations of the Nevada Consumer Fraud Act, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII in Defendant's custody in order to prevent incidents like the Data Breach from reoccurring in the future and for CAESARS to provide identity theft protective services to Plaintiff and Class Members for their lifetimes.

PARTIES

9. Plaintiff Oliver McCusker is an adult who, at all relevant times hereto, is a citizen and resident of the State of Nevada. Plaintiff received a notification email from CAESARS informing him that his PII in Defendant's possession had been compromised in the Data Breach.

10. Defendant CAESARS is a Delaware corporation with its principal place of business in Nevada. CAESARS is a citizen of the States of Delaware and Nevada.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess

---

[4] *Id.*

[5] *Id.*; https://response.idx.us/Caesars/#learn-more (last visited Oct. 27, 2023).

of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

12. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

13. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL BACKGROUND

CAESARS Collected and Stored Plaintiff's and Class Members' PII.

14. CAESARS is a global entertainment company with numerous iconic locations along the Las Vegas Strip, and locations in other cities within the United States, including Arizona, California, Colorado, Florida, Illinois, Indiana, Iowa, Louisiana, Maryland, Mississippi, Missouri, Nevada, New Jersey, North Carolina, Ohio, and Pennsylvania.[6]

15. CAESARS offers its customers "the finest restaurants, the biggest entertainment, elite meeting and conventions facilities, and unparalleled shopping."[7]

16. CAESARS prides itself on being the largest gaming company in the United States. It also runs one of the largest casino loyalty programs in the United States with over 60 million members, which it calls Caesars Rewards.[8]

17. Upon information and belief, in the course of doing business with CAESARS, customers who wish to become Caesars Rewards members are required provide to provide their sensitive personal information to CAESARS, including their full name, contact information, driver's license number, and/or Social Security number.

---

[6] *Caesars Properties*, https://investor.caesars.com/caesars-properties (last visited Oct. 27, 2023).
[7] *This is Caesars: Who We Are*, https://www.caesars.com/corporate (last visited Oct. 27, 2023).
[8] https://www.Caesars.com/corporate; https://www.vegashowto.com/caesars-rewards (last visited Oct. 27, 2023).

18. CAESARS, in turn, provides special benefits to Caesars Rewards members in selling them its goods and services. The more that members spend on CAESARS's goods and services, the higher "Tier" of membership they can achieve.[9]

19. In return for the provision of this sensitive information to CAESARS, customers reasonably believe that CAESARS will safeguard their highly sensitive information from those who would use it for nefarious purposes.

20. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, CAESARS assumed equitable and legal duties to safeguard Plaintiff's and Class Members' highly sensitive information.

21. Despite these duties, however, CAESARS nevertheless employed inadequate data security measures to protect and secure the customer PII entrusted to it, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII.

CAESARS Knew the Risks of Storing Valuable PII and the Foreseeable Harm to Victims.

22. CAESARS was well aware that the PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

23. CAESARS also knew that a breach of its computer systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

24. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

25. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[10]

26. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and

---

[9] https://www.caesars.com/myrewards/benefits-overview; https://www.caesars.com/content/dam/caesars-rewards/benefits/2023-07-cr-flipbook-reprint-czr.pdf (last visited Oct. 27, 2023).

government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[11]

27. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[12]

28. The hospitality industry has become a prime target for threat actors. A report by Cornell University and Freedom Pay found that "[n]early 31 percent of hospitality organizations have reported a data breach in their company's history, of which 89 percent have been affected more than once in a year."[13] Indeed, businesses in the hospitality sector are targeted by cybercriminals because they must balance guest satisfaction and reputation against staying secure.[14]

29. The hospitality sector also faces unique cybersecurity risks as the nature of the industry "means a high turnover of staff, and more difficulty means a high turnover of staff, and more difficulty to keep on top of security training."[15] Further, because a hospitality business "serves hundreds of different customers on a daily basis, this means providing a network and bandwidth secure and large enough to keep up with the sheer number of users, while at the same time making businesses hesitant to deploy any patches and configuration changes as it may have an impact on the day-to-day operations."[16]

---

[10] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[11] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[12] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Oct. 27, 2023).

[13] Esther Hertzfeld, *Report: 31% of hospitality organizations have had a data breach*, Hotel Management (Sept. 8, 2023), https://www.hotelmanagement.net/tech/report-31-hospitality-organizations-have-had-data-breach.

[14] Nicole Deslandes, *Over a third of hospitality organizations have reported a data breach*, Tech Informed (Sept. 8, 2023), https://techinformed.com/over-a-third-of-hospitality-organisations-have-reported-a-data-breach/.

[15] *Id.*

[16] *Id.*

30. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves CAESARS's customers especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

31. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

32. The Social Security Administration even warns that the process of replacing a Social Security is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[17]

33. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of

[17] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

34. **Driver's License Numbers—**are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive. This is because a driver's license number is connected to an individual's vehicle registration, insurance policies, records on file with the DMV, places of employment, doctor's offices, government agencies, and other entities.

35. For these reasons, driver's license numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

36. Further, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of PII at stake here—unique driver's license numbers—cannot be easily replaced.

37. The ramifications of CAESARS's failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[18]

38. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and

[18] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Oct. 20, 2023).

affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

39. Based on the value of its customers' PII to cybercriminals, CAESARS knew or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. CAESARS, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

CAESARS Owes a Duty to Safeguard its Customers' PII.

40. CAESARS has a responsibility to securely maintain the customer PII that it receives and keep it safe from harm.

41. CAESARS expressly recognizes this duty, stating it its Privacy Policy it is "committed to respecting your data privacy" and that it maintains "physical, electronic, and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of information under our control."[19]

42. Despite its assurances, CAESARS failed to maintain the necessary security measures, practices, and other safeguards that would have prevented the Data Breach.

43. CAESARS knew that the massive databases of PII it collected, processed, and stored were tantalizing targets for hackers. [20]

44. Hotel and hospitality companies are particularly attractive targets for financially-motivated hackers looking steal PII. Trustwave's 2020 Global Security Report lists hospitality as the industry with the third largest share of security compromises and data breaches.[21] Indeed, "[t]he

---

[19] https://www.caesars.com/corporate/privacy (last visited Oct. 27, 2023).

[20] Identity Theft Resource Center, Identity Theft Resource Center's *2022 Annual Data Breach Report Reveals Near-Record Number of Compromises*, https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/ (last visited Oct. 27, 2023).

[21] 2020 Trustwave Global Security Report, https://21158977.fs1.hubspotusercontent-na1.net/hubfs/21158977/Web/Library/Documents%20pdf/D_16791_2020-trustwave-global-security-report.pdf (last visited Oct. 27, 2023).

hospitality industry is a common target for cyber criminals because of the massive amount of data hotels hold."[22]

45. Similarly, cybersecurity experts have described casinos as "obvious candidates" for cybercriminals as "[t]hey have money and their downtime costs are high, which may mean they're more likely to pay."[23] Indeed, casinos are attractive targets for cybercriminals because many "use 'flat' IT infrastructure, meaning that once hackers access a network, it's easy for them to burrow into accounting systems and customer credit card records before making a ransom demand."[24]

46. CAESARS was particularly aware that it was a prime target for data breaches because of past attacks affecting other large gambling enterprises. In July 2019, hackers gained unauthorized access to MGM's networks, successfully exfiltrating the PII of millions of MGM's customers.[25]

47. The Federal Trade Commission ("FTC") has promulgated various guides for businesses, which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[26]

48. In 2016, the FTC updated its publication titled Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.[27] The guidelines state that:

a. Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it";

---

[22] Open Data Security, *Cybersecurity in the Hotel Industry*: *Lessons from Marriott Data Breach*, https://opendatasecurity.co.uk/cybersecurity-in-the-hotel-industry-lessons-from-marriott-data-breach/ (last visited Oct. 27, 2023).

[23] Katrina Manson & William Turton, *A Casino Hack Throttles the Betting World*, Bloomberg, (Sept. 13, 2023), https://www.bloomberg.com/news/newsletters/2023-09-13/a-casino-hack-on-mgm-resorts-throttles-the-betting-world?sref=gni836kR.

[24] *Id.*

[25] *Id.*

[26] *See Start With Security: A Guide for Business*, Federal Trade Commission, June 2015, available at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business. (last visited Oct. 27, 2023).

[27] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission, October 2016, available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Oct. 27, 2023).

b. Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

d. Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

e. Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.

49. In another publication, the FTC recommended that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[28]

67. Notably, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Indeed, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

50. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

51. CAESARS was at all times fully aware of its obligations to protect the PII of its customers because of its position as a gaming and hospitality provider, which gave it access to reams of

[28] *See Start with Security: A Guide for Business*, Federal Trade Commission, June 2015, available at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business. (last visited Oct. 27, 2023).

customer PII. CAESARS was also aware of the significant repercussions that would result from its failure to do so.

52. Upon information and belief, CAESARS failed to properly implement one or more of the basic data security practices recommended by the FTC. CAESARS's failure to employ reasonable and appropriate data security measures to protect against unauthorized access to customers' PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act, and state statutory analogs.

53. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[29]

54. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[30] CAESARS failed to adhere to the NIST guidance.

55. Further, cybersecurity experts have identified various best practices that should be implemented by entities in the hotel industry, including the following:

a. Installing appropriate malware detection software;

b. Monitoring and limiting network ports;

c. Protecting web browsers and email management systems;

d. Setting up network systems such as firewalls, switches, and routers;

e. Monitoring and protecting physical security systems; and

f. Training hotel staff regarding critical points.

56. Upon information and belief, CAESARS's failure to protect massive amounts of PII is a result of its failure to adopt reasonable safeguards as required by the FTC guidelines, NIST guidance, and industry best practices.

---

[29] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, available at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (las visited Oct. 27, 2023).

[30] *Id.* at Table 2 pg. 26-43.

57. CAESARS was well aware of its obligations to use reasonable measures to protect consumers' PII. Caesars also knew it was a target for hackers, as discussed above. Despite understanding the risks and consequences of inadequate data security, CAESARS failed to comply with its data security obligations.

CAESARS's Breached its Duty to Safeguard Customer PII

58. Upon information and belief, during the course of its business operations, CAESARS engages OKTA for identity and access management services. OKTA offers cloud software to help clients manage and secure user authentication into applications.

59. On or about September 7, 2023, CAESARS filed an 8-K notice with the Securities and Exchange Commission ("SEC"), confirming a recent cyberattack. In its 8-K notice, CAESARS further indicated that cyberattack was the result of a successful social engineering attack at its IT support vendor (OKTA) that enabled cybercriminals to gain access to CAESARS's computer systems, including its loyalty program database.[31]

60. Upon information and belief, the Data Breach occurred as a result of the cybercriminals duping a CAESARS's IT service desk personnel into providing access to CAESARS computer networks by either (1) resetting passwords to an OKTA Super Administrator account or (2) requesting a rest of all Multi-Factor Authentication ("MFA") for an OKTA Super Administrator account.[32] After gaining access to an OKTA Super Administrator account, the cybercriminals were able to impersonate a CAESARS's account user, and gain access to CAESARS's computer network providing the cybercriminals with the opportunity to access and exfiltrate the sensitive customer information stored therein.

61. After detecting suspicious activity on its computer systems, CAESARS launched an investigation into the Data Breach a determined that the cybercriminals acquired, among other data, a

---

[31] *Form 8-K*, Caesars Entertainment, Inc. (Sept. 7, 2023), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001590895/000119312523235015/d537840d8k.htm.

[32] *Cross-Tenant Impersonation: Prevention and Detection*, okta (Aug. 31, 2023), https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection

copy of CAESARS' loyalty program database, which included sensitive PII, including customer names, driver's license numbers, and Social Security numbers.[33]

62. In response to a likely ransom demand, news outlets reported that CAESARS paid approximately $15 million to the cybercriminals to prevent the leak of the stolen customer PII.[34]

63. However, despite paying the ransom, CAESARS could not provide any assurances that the cybercriminals responsible for the Data Breach would not misuse the stolen PII, including later leaking or selling the stolen PII on the dark web.[35]

64. On or about October 6, 2023, CAESARS began notifying impacted customers of the Data Breach. While CAESARS has yet to report the full size of the Data Breach, it has indicated that the Data Breach impacted at least thousands of individuals.[36]

65. The social engineering attack that led to the Data Breach was readily preventable. OKTA has reported a pattern of social engineering attacks directed at its customers IT service desk personnel, "in which the caller's strategy was to convince service desk personnel to reset all [MFA] factors enrolled by highly privileged users." OKTA further indicated that such methods "are preventable and present several detection opportunities for defenders."[37]

66. During social engineering attacks, such as the one that lead to the Data Breach, an attacker will pose "as an individual with a legitimate need for information such as an IT worker who needs a person to 'verify their login credentials,' or a new employee who urgently needs an access token but doesn't know the proper procedure to acquire one."[38] Once the attacker has tricked a person into handing over access credentials, the attacker can then use that information to gain access to an entity's systems.

---

[33] *Form 8-K*, *supra* note 32.

[34] Sergiu Gatlan, *Caesars Entertainment confirms ransom payment, customer data theft*, BleepingComputer (Sept. 14, 2023), https://www.bleepingcomputer.com/news/security/caesars-entertainment-confirms-ransom-payment-customer-data-theft/.

[35] *Id.*

[36] *Data Breach Notifications*, *supra* note 3.

[37] *Tenant Impersonation: Prevention and Detection*, *supra* note 33.

[38] Bart Lenarerts-Bergmans, *What is Social Engineering?*, CrowdStrike (May 23, 2023), https://www.crowdstrike.com/cybersecurity-101/social-engineering/.

67. Companies with adequate cybersecurity measures will employ one or more of the following measures to guard against social engineering attacks:

a. Employ security awareness training to remind employees of common practices, including (1) being wary of emails or phone calls requesting account information, (2) not providing usernames, passwords, dates of birth, Social Security numbers, financial data, or other personal information in response to an email or robocall, (3) independently verify any requested information originating from a legitimate sort;

b. Employ cybersecurity solutions; and

c. Employ zero trust architecture, limiting a user's access to specific systems to perform specific tasks, and only for a limited period of time.[39]

68. OKTA further recommends its clients, such as CAESARS, to implement the following cybersecurity measures to prevent successful social engineering attacks such as the one that lead to the Data Breach:

a. Enforce phishing-resistant authentication;

b. Require re-authentication for privileged application access;

c. Use strong authenticators for self-service and limit to trusted networks;

d. Enhance help desk verification with visual checks, MFA challenges, and manager approvals;

e. Activate and test alerts for new devices and suspicious activity;

f. Limit Super Administrator roles, implement privileged access management, and delegate high-risk tasks; and

g. Mandate administrators to sign-in from managed devices with phishing resistant MFA and limit access to trusted zones.

69. Upon information and belief, the Data Breach is the direct and proximate result of CAESARS's failure to implement on or more of the above data security measures.[40]

---

[39] *Id.*

[40] *Tenant Impersonation: Prevention and Detection*, *supra* note 33.

The Data Breach Harmed Individuals, And Additional Fraud Will Result

59. Consumers who have been victims of data breaches are much more likely to become victims of identity fraud than those who have not. Further, each additional data breach an individual is involved in increases his or her risk of identity fraud.

60. As the FTC explains, "[o]nce identity thieves steal your personal information . . . they can drain your bank account, run up charges on your credit cards, get new credit cards in your name, open a phone, cable, or other utility account in your name, steal your tax refund, use your health insurance to get medical care, or pretend to be you if they are arrested."[41] As such, PII is a highly valuable asset to ill-intending identity thieves.

61. The U.S. Department of Justice's Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims "reported spending an average of about 7 hours clearing up the issues."[42]

62. Data Breach victims who do experience identity theft often spend hundreds of hours fixing the damage caused by identity thieves.[43]

63. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone

---

[41] https://consumer.ftc.gov/articles/free-credit-reports (last visited Oct. 27, 2023).

[42] Erika Harrell, *Victims of Identity Theft*, 2014, NCJ 248991, September, 27, 2015, available at https://bjs.ojp.gov/content/pub/pdf/vit14.pdf (last visited at Oct. 27, 2023).

[43] Consumer Protection Division of the Maryland Office of the Attorney General, *Identity Theft: Protect Yourself, Secure Your Future*, https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf (last visited Oct. 27, 2023).

> illegally using your Social Security number and assuming your identity can cause a lot of problems.[44]

64. Therefore, information compromised in this Data Breach is more valuable than the loss of, for example, credit card information in a retailer data breach. There, victims can close credit and debit card accounts, typically for free. Here, the information compromised—Social Security numbers, drivers' license numbers, and names—cannot be "closed" and is difficult, if not impossible, to change.

65. While CAESARS is offering members of its rewards program members two years of free identity protection services, the identity protection services CAESARS is offering are inadequate. In fact, identity thieves often hold onto personal information in order to commit fraud years after such free programs expire. Moreover, the services CAESARS is offering fail to actually prevent identity theft. At best, they can report after the theft occurs. Moreover, the insurance and other benefits that CAESARS offers is insufficient, full of coverage loopholes, and very difficult to successfully claim.

66. In addition to a remedy for economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their PII, which remains in CAESARS' computer systems, systems that have proved vulnerable to compromise, is secure, remains secure, and is not subject to further misappropriation and theft.

Plaintiff's Experience.

68. Plaintiff was a customer at one or more of CAESARS's resorts. Plaintiff is also a member of CAESARS loyalty program. In order to do business with CAESARS, Plaintiff was required to entrust CAESARS with his PII and, in return, reasonably expected that CAESARS would safeguard his PII from unauthorized access. On or about October 19, 2023, however, Plaintiff received an email notification from CAESARS informing him that his PII in CAESARS's possession had been compromised in the Data Breach.

69. CAESARS has offered Plaintiff little remedial measures to protect his PII going forward, other than stating it had arranged with Experian to offer Plaintiff credit monitoring and identity protection services for two years. This offer is time-limited and will expire long before the threat to Plaintiff's PII is exhausted. CAESARS also put the onus on Plaintiff to protect his PII, "recommend[ing]

---

[44] Social Security Administration, *Identity Theft and Your Social Security Number*,

that [he] remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring [his] free credit reports."[45] CAESARS further "recommend[ed] that [Plaintiff] remain alert for unsolicited communications involving [his] personal information."[46]

70. Plaintiff has suffered actual injury from having his PII exposed and/or stolen as a result of the Data Breach, including: (1) required mitigation efforts, including needing to monitor his financial and other accounts to ensure his information is not used for identity theft and fraud; (b) damages to and diminution of the value of his PII, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; and (c) loss of privacy.

71. In addition, knowing that hackers accessed and likely exfiltrated his PII and that this information likely has been and will be used in the future for identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

72. As a direct and proximate result of the Data Breach, Plaintiff has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending, and is not speculative, given the highly sensitive nature of the PII compromised in the Data Breach.

Plaintiff and Class Members Have Suffered Damages.

73. For the reasons mentioned above, CAESARS's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways, including actual fraud as well as substantial and imminent risk of identity theft and fraud. Plaintiff and Class Members must immediately devote time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering, spear phishing, or extortion attacks; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

---

https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 27, 2023).

[45] *Data Breach Notifications*, *supra* note 3.

74. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of CAESARS's conduct. Further, the value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach.

75. As a result of CAESARS's failures, Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

76. Indeed, PII is a valuable commodity to identity thieves, and, once it has been compromised, criminals will use them and trade the information on the cyber black market for years thereafter. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[47] Similarly, Trustwave has indicated that passports and driver's licenses can sell between $1-$50 on the dark web. [48]

77. The reality is that cybercriminals seek nefarious outcomes from a data breach and stolen PII can be used to carry out a variety of crimes.

78. Plaintiff and Class Members are also at a continued risk because their information remains in CAESARS's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as CAESARS fails to undertake the necessary and appropriate security and training measures to protect its customers' PII.

79. Plaintiff and Class Members have lost the benefit of their bargains. Plaintiff and Class Members entered into agreements with and provided payment to CAESARS under the reasonable but

---

[46] *Id.*

[47] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10xprice-of-stolen-credit-card-numbers.html.

[48] *The Price Cybercriminals Charge for Stolen Data*, Trustwave (Aug. 6, 2023), https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-price-cybercriminals-charge-for-stolen-data/.

mistaken belief that it would reasonably and adequately protect their PII. Plaintiff and Class Members would not have entered into such agreements and would not have paid CAESARS the amount that they paid had they known that CAESARS would not reasonably and adequately protect their PII. Plaintiff and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the services that include reasonable and adequate data security that they bargained for, and the services that do not, which they actually received.

80. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers and cybercriminals.

CLASS ACTION ALLEGATIONS

81. Plaintiff brings this class action on behalf of himself and all others who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

82. Plaintiff seeks to represent the following Class of persons defined as follows:

> All individuals in the United States whose PII was compromised in the CAESARS Data Breach which was announced on or about September 7, 2023 (the "Class").

83. Excluded from the Class is Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

84. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

85. **Numerosity:** The members of the Class are so numerous that the joinder of all members is impractical. Plaintiff is informed and believes, and thereon alleges, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through CAESARS's records, including but not limited to the files implicated in the Data Breach.

86. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether CAESARS had a duty to protect the PII of Plaintiff and Class Members;

b. Whether CAESARS was negligent in collecting and storing Plaintiff's and Class Members' PII, and breached its duties thereby;

c. Whether CAESARS entered into contracts implied in fact with Plaintiff and the Class;

d. Whether CAESARS breached those contracts by failing to adequately safeguard Plaintiff's and Class Members' PII;

e. Whether CAESARS's conduct is violative of the Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600;

f. Whether Plaintiff and Class Members are entitled to damages as a result of CAESARS's wrongful conduct; and

g. Whether Plaintiff and Class Members are entitled to restitution as a result of CAESARS's wrongful conduct.

87. **Typicality:** Plaintiff's claims are typical of the claims of Class Members. Plaintiff's and Class Members' claims are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and Class Members were all customers of CAESARS, each having their PII exposed and/or accessed by an unauthorized third party.

88. **Adequacy:** Plaintiff is an adequate representative of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

89. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of

scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

90. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

91. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that generally apply to the Class making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23(b)(2).

92. **Ascertainability:** Class Members are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through CAESARS's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(Plaintiff on Behalf of the Class)

93. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

94. Plaintiff brings this claim individually and on behalf of the Class.

95. CAESARS owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty including, among other things: (a) designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class Members' PII in CAESARS's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

96. CAESARS's duty to use reasonable care arose from several sources, including but not limited to those described below.

97. CAESARS had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by cybercriminals for unauthorized access, CAESARS was obligated to act with reasonable care to protect against these foreseeable threats.

98. CAESARS also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiff and Class Members. CAESARS's conduct included its failure to adequately restrict access to its computer networks that held customers' PII.

99. CAESARS also knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII, and the frequency of cyberattacks such as the Data Breach in the hospitality sector.

100. Further, CAESARS's duty arose from various statutes requiring Defendant to implement reasonable data security measures, including but not limited to: Section 5 of the FTC Act and Nev. Rev. Stat. § 603A.210. For example, Section 5 of the FTC Act required Defendant to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Defendant's duty to Plaintiff and the Class. Section 5 of the FTC Act prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to use reasonable measures to protect highly sensitive data. Therefore, Defendant was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendant's duties to adequately protect sensitive information. By failing to implement reasonable data security measures, Defendant acted in violation of Section 5 of the FTC Act.

101. CAESARS is subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and Defendant and Class Members. The sources of CAESARS's duty are identified above.

102. CAESARS's violation of Section 5 of the FTC Act, and state data security statutes constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff and Class Members belong and to prevent the type of harm that resulted from the Data Breach.

103. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies provided to its customers; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

104. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised and or exfiltrated from CAESARS's computer systems.

105. As a direct and proximate result of CAESARS's negligence, Plaintiff and Class Members have suffered injuries, including: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

106. As a direct and proximate result of CAESARS's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, damages in an

amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Plaintiff on behalf of the Class)

107. Plaintiff restates and realleges all preceding allegations set forth above as if fully alleged herein.

108. Plaintiff brings this claim individually and on behalf of the Class.

109. When Plaintiff and Class Members provided their PII to CAESARS in exchange for gaming and hospitality services, including loyalty program benefits, they entered into implied contracts with Defendant, under which CAESARS agreed to take reasonable steps to protect Plaintiff's and Class Members' PII.

110. CAESARS solicited and invited Plaintiff and Class Members to provide their PII, including their names, driver's license numbers, and Social Security numbers in order to become loyalty program members. Plaintiff and Class Members accepted CAESARS's offers and provided their PII to Defendant.

111. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that CAESARS employed adequate data security measures to safeguard their PII. Implicit in the agreement between Plaintiff and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) to prevent unauthorized disclosures of the PII; (d) to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (e) to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses; and (f) to retain the PII only under conditions that kept such information secure and confidential.

112. Plaintiff is informed and believes that in Defendant's written privacy policies, CAESARS expressly promised Plaintiff and Class Members that Defendant would implement reasonable data security measures to protect their PII, including storing PII on systems protected by industry standard security measures and training to staff to take reasonable measures to ensure that unauthorized person cannot view or access PII.[49] Plaintiff and Class Members paid money to CAESARS in the form of

[49] https://www.caesars.com/corporate/privacy (last visited Oct. 27, 2023).

monies made for payments in order to receive gaming and hospitality services. Plaintiff and Class Members reasonably believed and expected that CAESARS would use part of those funds to obtain adequate data security. CAESARS failed to do so.

113. Plaintiff and Class Members would not have provided their PII to Defendant had they known that CAESARS would not safeguard their PII as promised.

114. Plaintiff and Class Members fully performed their obligations under their implied contracts with CAESARS.

115. CAESARS breached its implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' PII.

116. The losses and damages Plaintiff sustained, include, but are not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

117. As a direct and proximate result of CAESARS's breach of implied contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
VIOLATION OF THE NEVADA CONSUMER FRAUD ACT
Nev. Rev. Stat. § 41.600
(Plaintiff on Behalf of the Class)

118. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

119. Plaintiff brings this claim individually and on behalf of the Class.

120. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600 states in relevant part:

> An action may be brough by any person who is a victim of consumer fraud. As used in this section, "consumer fraud" means: . . . A deceptive trade practice defined in NRS 598.0915 to 598.0225, inclusive.
>
> Nev. Rev. Stat. § 41.600(1) & (2)(e).

121. In turn, Nev. Rev. Stat. § 598.0923(2) provides that "[a] person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly . . . [f]ails to disclose a material fact in connection with the sale or lease of goods or services." *Id.* CAESARS violated this provision because it failed to disclose the material fact that its data security measures were inadequate to reasonably safeguard its customers' PII. This is true because, among other things, CAESARS was aware that the hospitality sector is a frequent target of cyberattacks such as the Data Breach. CAESARS knew or should have known that that its data security measures were insufficient to guard against attacks such as the Data Breach. CAESARS had knowledge of the facts that constituted the omission, CAESARS could have and should have made a proper disclosure when accepting new customers, while providing its goods and services to customers, or by any other means reasonably calculated to inform customers of its inadequate data security measures.

122. Further, Nev. Rev. Stat. § 598.0923(3) provides that "[a] person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly . . . [v]iolates a state or federal statute or regulation relating to the sale or lease of goods or services." *Id.* CAESARS violated this provision for several reasons, each of which serves as an independent basis for violating Nev. Rev. Stat. § 598.0923(3).

123. First, CAESARS breached its duty under Nev. Rev. Stat. § 603A.210, which requires any data collector "that maintains records which contain personal information" of Nevada residents to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." *Id.* CAESARS is a "data collector" as defined by Nev. Rev. Stat. § 603A.030. CAESARS failed to implement such reasonable security measures, as shown by a system-wide breach of its computer systems during which a threat actor exfiltrated customer PII. CAESARS's violation of this statute was done knowingly for the purposes of Nev. Rev. Stat. §

598.0923(3) because CAESARS knew or should have known that the hospitality sector is a frequent target of cyberattacks such as the Data Breach. CAESARS knew or should have known that its data security measures were inadequate to protect against cyberattacks such as the Data Breach.

124. Second, CAESARS violated Section 5 of the FTC Act, as alleged above. CAESARS knew or should have known that its data security measures were inadequate, violated Section 5 of the FTC Act, and failed to adhere to the FTC's data security guidance. This is true because CAESARS was well aware that the hospitality sector is a frequent target of cyberattacks such as the Data Breach and the FTC has recommended various data security measures that companies such as Defendant could have implemented to mitigate the risk of a Data Breach. CAESARS chose not to follow such guidance and knew or should have known that its data security measures were inadequate to guard against cyberattacks such as the Data Breach. CAESARS had knowledge of the facts that constituted the violation. CAESARS's violation of Section 5 of the FTC Act serves as a separate actional basis for purposes of violating Nev. Rev. Stat. § 598.0923(3).

125. CAESARS engaged in an unfair practice by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiff and Class Members.

126. Plaintiff and members of the Class were denied a benefit conferred on them by the Nevada legislature.

127. As a direct and proximate result of the foregoing, Plaintiff and Class Members have suffered injuries including, but not limited to actual damages, and in being denied a benefit conferred on them by the Nevada legislature.

128. As a result of these violations, Plaintiff and Class Members are entitled to an award of actual damages, equitable injunctive relief requiring Defendant to implement adequate data security measures, as well as an award of reasonable attorney's fees and costs. Nev. Rev. Stat. § 41.600(3).

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiff on behalf of the Class)

129. Plaintiff restates and realleges all preceding allegations set forth above as if fully alleged herein.

130. Plaintiff brings this claim individually and on behalf of the Class.

131. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

132. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether CAESARS is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

133. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that, among other things:

a. CAESARS owed a legal duty to secure customers' PII under the common law, Section 5 of the FTC Act, and state data security laws; and

b. CAESARS breached and continues to breach this legal duty by failing to employ reasonable measures to secure customers' PII.

134. This Court also should issue corresponding prospective injunctive relief requiring CAESARS to employ adequate security protocols consistent with law and industry standards to protect customers' PII.

135. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at CAESARS. The risk of another such breach is real, immediate, and substantial. If another breach at CAESARS occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

136. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to CAESARS if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to CAESARS of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and CAESARS has a pre-existing legal obligation to employ such measures.

137. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at CAESARS, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and consumers whose confidential information would be further compromised.

DEMAND FOR JURY TRIAL

Please take notice that Plaintiff demands a trial by jury as to all issues so triable in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all other similarly situated, prays for relief as follows:

1. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

2. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

3. For compensatory damages on behalf of Plaintiff and the Class;

4. For punitive damages on behalf of Plaintiff and the Class;

5. For an order of restitution and all other forms of equitable monetary relief;

6. Declaratory and injunctive relief as described herein;

7. For disgorgement and/or restitution as the Court deems appropriate, just, and proper;

8. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

9. Awarding pre- and post-judgment interest on any amounts awarded;

10. For reimbursement for all costs and expenses incurred in connection with the prosecution of these claims; and

11. Awarding such other and further relief as may be just and proper.

Dated this 3rd day of November 2023.

THE BOURASSA LAW GROUP

/s/ Jennifer A. Fornetti

MARK J. BOURASSA, ESQ. (NBN 7999)
JENNIFER A. FORNETTI, ESQ. (NBN 7644)
VALERIE S. GRAY, ESQ. (NBN 14716)
2350 W. Charleston Blvd., Suite 100

Las Vegas, Nevada 89102

GARY F. LYNCH
(*pro hac vice forthcoming*)
PATRICK D. DONATHEN
(*pro hac vice forthcoming*)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Attorneys for Plaintiff